# STATE OF ALABAMA

## Information Technology Standard

**Standard 640-01S2: Secure Web Application Deployment**

### 1. INTRODUCTION:

State agencies are increasingly utilizing applications that require data to be accessed via the Internet. Many of these applications require web servers to be publicly accessible while at the same time providing data access from secure servers within the State network. If deployed improperly, these applications can open up backdoors to the State network by allowing unauthorized users access to trusted State network resources.

There are methods to securely deploy such applications. By utilizing a combination of secure application gateways, firewalls, application code review/application security assessments, configuration and change control procedures, Internet accessible segments (IAS) and multiple server configurations, the State can deploy secure web applications with a reduced risk to State network resources.

### 2. OBJECTIVE:

Define the requirements for secure deployment of web applications.

### 3. SCOPE:

These requirements apply to system owners, data owners, program managers, security officers, system architects, system administrators, and network administrators who are responsible for planning, approving, or establishing web application deployments.

### 4. REQUIREMENTS:

4.1 COMMON SECURITY MEASURES

A Secure Application Gateway shall be placed in front of the web server. A Secure Application Gateway, which is essentially a Layer Seven firewall, will help prevent both common and higher level attacks against the web application.

Before any web application is considered for placement on the Internet, it shall be audited by ISD or an agent thereof for known security vulnerabilities (e.g., cross-site scripting, SQL Injection, session hijacking, etc.). Conduct a thorough assessment and code review of the application and database from both the client's and the developer's point of view.

Implement host and network based intrusion detection systems (IDS) and/or intrusion prevention systems (IPS) in accordance with State standards as part of the overall solution.

Logging, antivirus, host-based firewalls, and a documented vulnerability management process shall also be included as part of any web application deployment.

## 4.2 SCENARIO SPECIFIC SECURITY MEASURES

Appropriate implementation of one of the following four deployment architectures, combined with the common security measures (above), will minimize the threat of security compromises of State resources and sensitive data while enabling critical business functions.

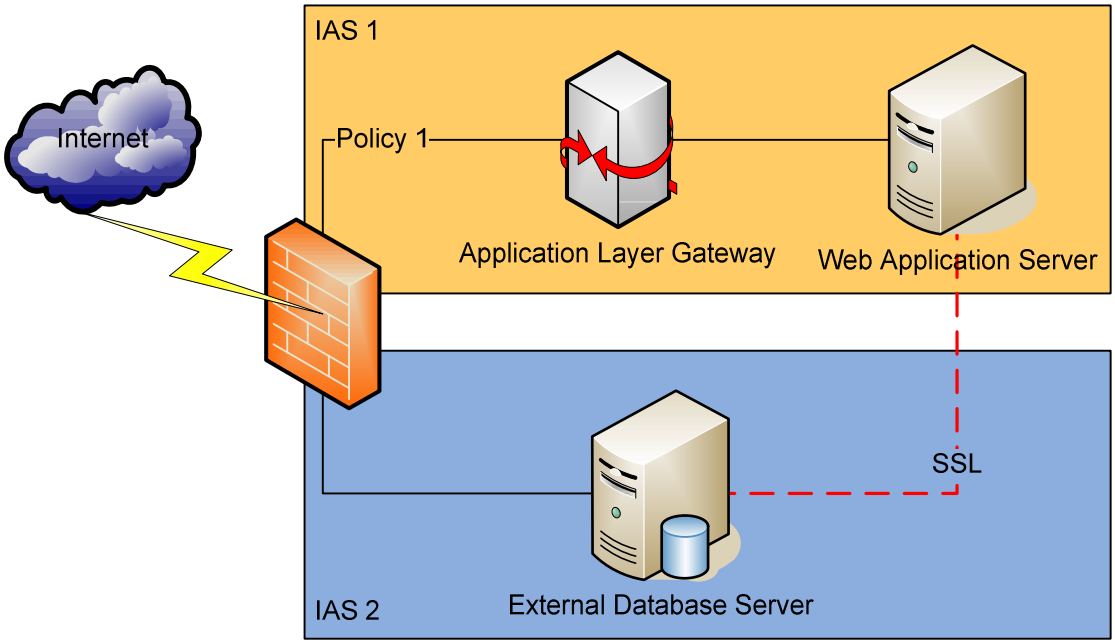
### 4.2.1 Scenario 1: A web application is placed on the Internet and requires access to its own database

This implementation uses a web server in front of a standalone database server.

The web server shall be configured to exclude all unnecessary applications and services, and be secured following applicable State standards. The server will be placed in an IAS with the Secure Application Gateway providing the initial protection. The firewall policy shall be set to only allow inbound HTTP (Port 80) and, if required, HTTPS (Port 443) (Policy 1).

The database server shall also be configured to exclude all unnecessary applications and services, and be secured in accordance with State standards. The database server will be deployed in a separate IAS. Secure Socket Layer (SSL) shall be used to encrypt the communication between the web server and the database server on a nonstandard port (see Figure 1: Web Application).

**Figure 1: Web Application**

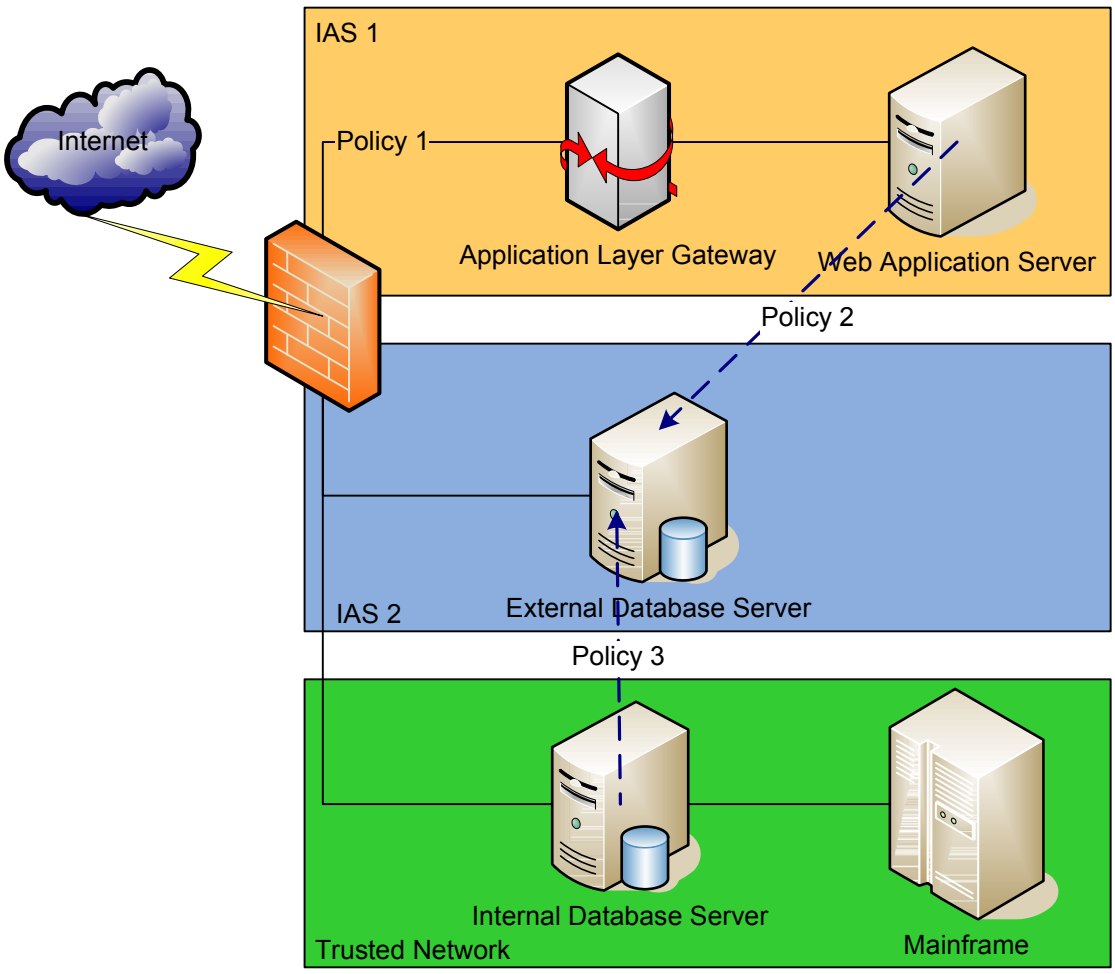



### 4.2.2 Scenario 2: A web application is placed on the Internet and needs access to an internal database (e.g. MS SQL or mainframe)

Secure the web server as in Scenario 1 (above).

A second database server will be placed as a buffer between the internal database server and the external web server. If mainframe access is required, the internal database server will have an agent installed, such as TC Access, to communicate directly with the mainframe (to prevent a compromised external database server from having direct access to the mainframe). Both the external and internal database servers shall be configured to exclude all unnecessary applications and services, and be secured in accordance with State standards. Secure Socket Layer (SSL) shall be used to encrypt the communication between the web server and the database server. The internal database server will be configured as a merge replication publisher and located on the internal (trusted) network. The external database server should be configured for replication as a subscriber and will be placed in an IAS. A policy shall be set to only allow inbound connections from the specific external web server to the specific external database server on a non-standard port (Policy 2). Another policy shall be configured to only allow inbound connection from the specific internal database server to the specific external database server on a non standard port (Policy 3) (see Figure 2 Internal Database Design).

**Figure 2: Internal Database Design**

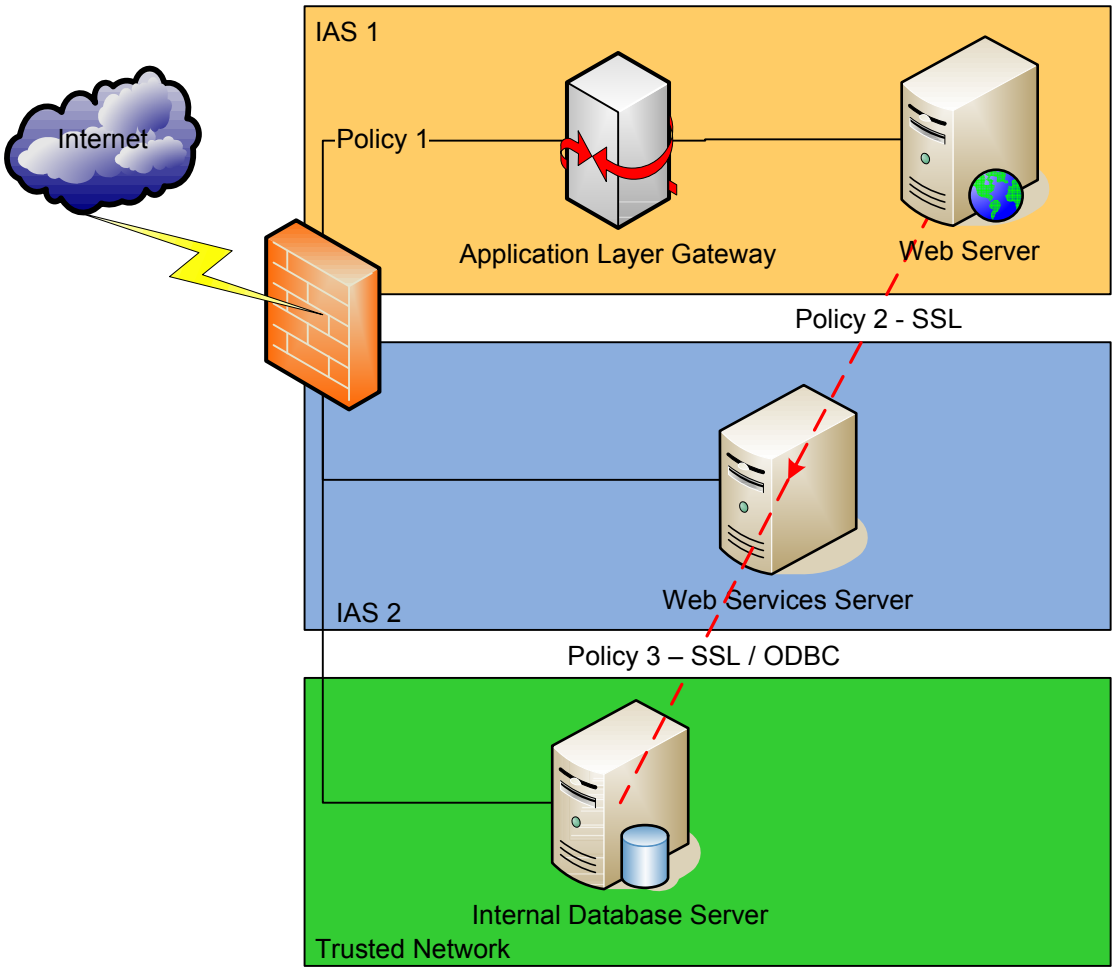


Using Microsoft SQL Server's Replication technology requires a SQL account be created on all servers participating in the replication with the same username and password. In addition these accounts must be granted full database access to the databases being replicated, placed in the System Administrator, Bulk Insert Administrator, and Process Administrator roles, resulting in a potential security risk. However, in replication the publisher establishes the connection to the subscribers to replicate the differences and Policy 3 would block any attempts to initiate a connection from the external database server. Proper logging should notify an administrator of attempted connections. If needed, the database servers can be configured to perform Transactional database replication (essentially real time data transfer).

### 4.2.3 Scenario 3: Use of Web Services

In either of the previous two scenarios, Web Services can additionally be utilized to give un-trusted users access to an internal database from the Internet. Web services were developed to provide application programming interfaces for systems that are not typically accessed via the Web. With web services, a client makes a request to a machine in an IAS which in turn establishes a connection to a server in a second IAS configured with the Web Services service. That machine then makes an ODBC (or a similar remote procedure call, RPC) connection to an internal database for the data query (see Figure 3 Web Services Design).

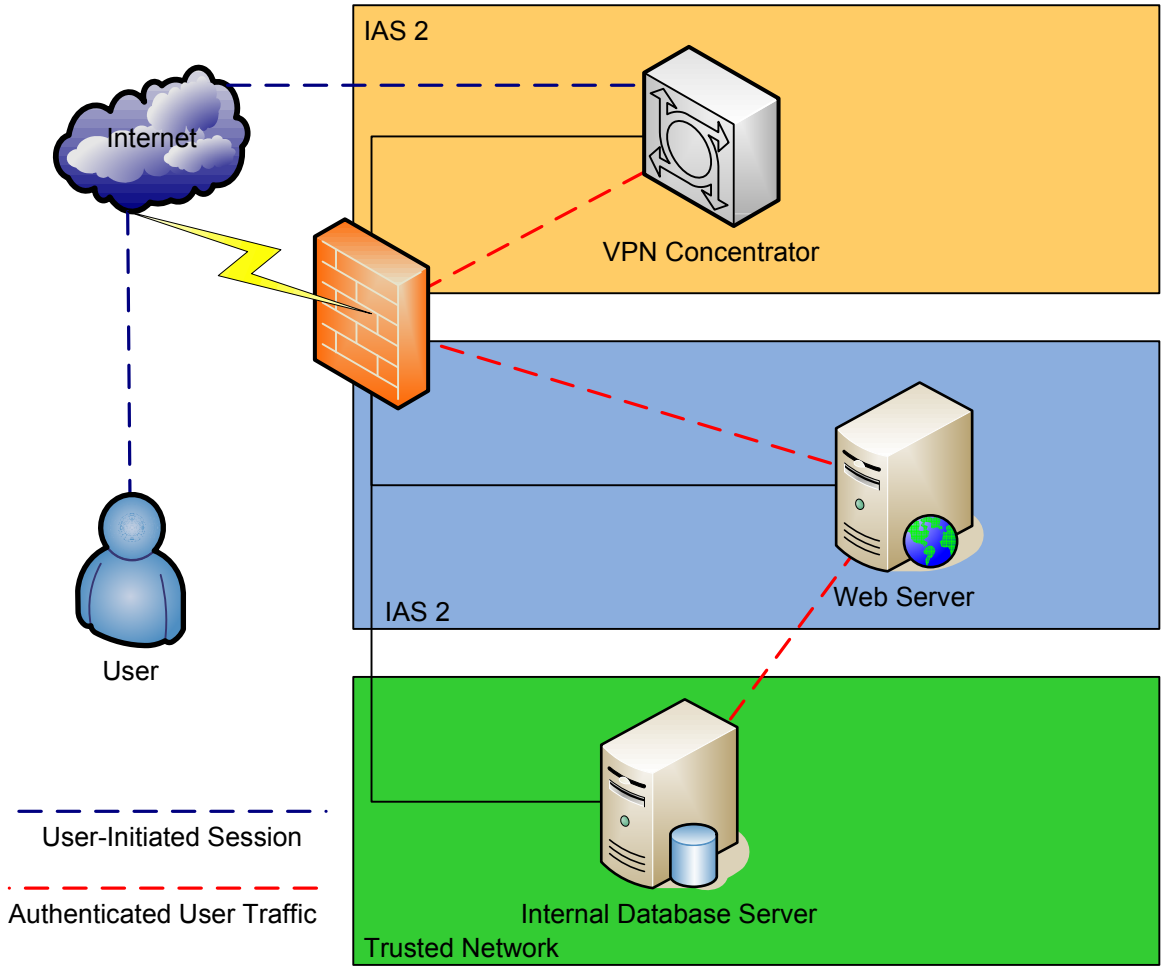
**Figure 3: Web Services Design**



### 4.2.4 Scenario 4: Trusted users are granted access to a database driven web application with the use of a Secure Socket Layer Virtual Private Network (SSL VPN)

With an SSL VPN connection, users are permitted access to an internal application by utilizing a secure (https) browser session, which is terminated at a VPN concentrator appliance. Users are authenticated to the network based on account information in the VPN concentrator appliance (which may authenticate against directory sources, such as Active Directory). The user's network access can also be restricted based on their user level, role or responsibility. This allows administrators to grant users access only to applications and data needed and not the entire network. Using a secure browser session eliminates the need for VPN client software. This also eliminates the need for multiple servers and multiple IASs which are needed with the other web application architectures (see Figure 4 SSL VPN Design).

**Figure 4: SSL VPN Design**



## 5. DEFINITIONS:

## 6. ADDITIONAL INFORMATION:

6.1 POLICY

Information Technology Policy 640-01: External Connections

6.2 RELATED DOCUMENTS

Information Technology Standard 640-01S1: Interconnecting IT Systems

Information Technology Policy 660-01: Application Security

*Signed by Jim Burns, Chief Information Officer*

## 7. DOCUMENT HISTORY:

| Version | Release Date | Comments |
|---|---|---|
| Original | 5/29/2007 | |
| | | |
| | | |